EXHIBIT 3

Affidavit of Joseph Nicholls

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
V.	)	Crim. No. 15-cr-10271-WGY
ALEX LEVIN	)	

AFFIDAVIT OF COMPUTER EXPERT JOSEPH NICHOLLS, NEED FOR ADDITIONAL DISCOVERY

I, Joseph Nicholls, state that the following is true to the best of my knowledge, information, and belief:

1. I am the principal and founder of Nicholls Data Recovery, LLC. in Gloucester, Massachusetts, which provides computer and cellphone digital forensic examination services to lawyers in the New England area.

2. I am a professionally trained, digital forensic examiner and have worked in the field of design and implementation of commercial computer, communication and information technology systems since 1974.

3. I have been retained to provide digital forensic services to the defense team for the above titled case.

4. From my education, training and experience I know that any software system has the possibility to calculate correct results as well as calculate erroneous results if certain sets of exception conditions exist. The normal computer software development process consists of designing the desired behavior of the software, creating that software and then testing that software before it is used in a production environment. Most professionally created software systems goes through some level testing called “Quality Assurance” (QA) or “Quality Control” (QC).

5. Most QA processes will check to make sure the software does what it is supposed to do. This testing is usually done under the conditions that everything is as it is supposed to be. Proper QA processes however, will also check to make sure that the software operates

correctly when something goes wrong.[1] This QA testing – called black box testing – requires the testers to think of every possible condition or exception that can come up in a production use situation. The most comprehensive QA processes tests for every possible condition or exception even if the testers cannot think of them. This QA testing – called white box testing – test each part (module) of the software with special testing software that programmatically generates all possible inputs (even though the testers might not be able to think as to why such an input would occur.)

6. The "Network Investigative Technique" (NIT) is not described in any of the discovery documentation I have reviewed. From my education, training, and experience I know that such techniques that could be used in a computer networking environment need to rely almost exclusively on software, some of which is commercially available and some of which has to be custom software development.

7. The paragraphs below list my suggestions to the defense team for additional discovery and my rational for each request. This rational is based on my education and training in computer design and development as well as my experience of 40 plus years designing, developing, managing and deploying commercial computer system software.

8. Below the term "value" or "values" is used to mean the content of the actual data. For example, if a computer has a NETBIOS name of "ForensicWS-1", we would say that the NETBIOS name has a value of "ForensicWS-1". When the term "NIT logged values" is used, it means the content of the data that the NIT is saving – such as if the NIT logs a public IP address of 108.20.181.106, it can be said that the public IP address logged byt the NIT had a value of "108.20.181.106".

9. The "full raw NIT result files" which include the IP address (or addresses) attributed to Mr. Levin.
This is so I can analyze if there is a pattern to the addresses collected which may reveal anomalies about the collection methods. Additionally, to compare the NIT logged values to the actual data on Mr. Levin's computer.

10. The "listing of all the data items that the NIT can possibly collect" whether or not they were actually collected in the data attributed to Mr. Levin's case.
This is so I can then compare all the values the NIT captured to the values stored on the subject computer. For example, there can be multiple IP addresses in a user's computer which may or may not have been the actual IP address used by that computer for any particular communication at any particular time.

11. The "listing of all the data item source locations", such as path and filenames, data

[1] Correct operation of software when something goes wrong is usually defined as the software retrying an operation or recording and/or notifying the something has gone wrong and the results are either not provided or annotated as not being usable.

structures, network communication packet fields, etc. as well as where the listed data items could possibly have been collected from, such as subject computer, server computer, network sniffer, router logs, etc. Where exactly is the NIT getting the data it is collecting?
This is so I can then compare all the data item values the NIT captured to the values in those locations on the actual computer.

12. Continuing from the above paragraph, it is not clear from the existing government discovery which of the many possible data structures in a user's computer is the NIT software using to get the public facing IP address and other data the NIT software is collecting. The common IP address of the user's computer will be the "private" IP (behind the router) and there can be one for a hard-wired connection and a different but simultaneous one for a WiFi connection. However, the public IP address (in front of the router) is the IP address that is needed to issue a search warrant to an internet service provider. Where is the NIT getting that public IP value? There are many IP address values stored in a computer that may be historic and not the current value in use. Thus, it is important to understand the exact location or locations each of these values are being obtained from. Another example, is the NIT getting the computer name from one of the Windows NT "\ControlSetxxx\ Control\ ComputerName\ ComputerName registry keys" or from computer's NETBIOS name which may or may not be the same?

13. The "List of all IP Addresses discovered via Pacifier."
This is needed to see if there is a pattern of the IP addresses which reveal anomalies about the collection methods.

14. The "Affidavit attached to the subpoena to Comcast."
The discovery file "Administrative_Subpoena_%23149055_and_Verizon_return.pdf" states a subpoena was issued to Comcast for 64 Plymouth Drive, Norwood. Mr. Levin's interview said Fios was the service provider yet the IP address captured was Verizon's. The residential search warrant affidavit also says the FBI knew it was a Verizon IP address.

15. "All the data used and the original sources of the data used as well as the algorithm used by the NIT software to create the unique NIT ID" which was used to relate the NIT collected information to a single computer over time.
This is needed to see if the data used and the method the data was collected may have some exception conditions that would result in non-unique IDs being created.

16. The "exact target URL (Uniform Resource Locator) a TOR user would have to enter into a TOR browser to get to the TOR Playpen server."
This is to see if there are any matching strings on the subject computer, either in file slack, unallocated space, paging/hibernation space or cache/database files.

17. “Mr. Levin’s ISP (FiOS) service provider records and account logs.”
This is to compare service provider recorded online activity to the NIT captured data and to compare with the log files on the subject computer.

18. The “List of any seized Onion Routers that Mr. Levin's alleged Playpen activity went through.”
This is to compare any TOR router information during Playpen activity with any digital artifacts in the subject computer that would indicate any Tor Circuit connections known to be connected to Playpen activity.

19. The “List of other covert NIT IP collections that were taking place at the same time that the residential search warrant affidavit states that Playpen activity data was being collected by the NIT.”
This is to see if any other NIT Tor surveillance operations were also sending data to the same government collection computer and can any patterns be detected to indicate if other surveillance activity got mixed up in this Pacifier data.

20. A “List of all the software code” used by the NIT during the time period discussed in the residential search warrant affidavit.
This is to get a road map and process flow as to what software modules used by the NIT is commercial software and what modules contain custom coding (either created by the government or under contract/direction by the government) used in support of the NIT.

21. The “Source code, include modules, macros, list of compilation and linking tools and instructions for compiling and linking any software used in the support of the NIT that is not listed as commercial software, used by the NIT during the time period discussed in the residential search warrant affidavit.”
This is to allow for a source code review of the custom NIT software to validate that the actual implementation software does indeed implement the items defined in the “Lists” requested above. For example, this allows me to validate that the data items the NIT can possibly collect” from paragraph 9 above is indeed the items and only these items are the ones collected.

22. The requested discovery materials are necessary to conduct a complete evaluation to verify the Government’s claims and the accuracy of those claims.

Signed under the pains and penalties of perjury, this 16th day of November, 2018.

Joseph Nicholls